

CLAIMS:

1. A method for a key to selectively allow access to an enclosure via wireless simultaneous transfer of data and of power, the enclosure being identified by an enclosure identification and having an enclosure lock controlled by a lock controller, the key and the lock controller in two-way communication for transmitting and receiving variable signals for validating that the key is authorized to access the enclosure, the variable signals transmitted between the key and the lock controller deterring detection and duplication to prevent unauthorized access to the enclosure, the method comprising:

a) transmitting an access request signal identifying the key from the key to the lock controller;

b) receiving by the key, a variable interrogation signal from the lock controller, in response to the access request signal;

c) decoding the variable interrogation signal to determine an enclosure identification and identify a variable interrogation question, the variable interrogation question corresponding to one of a plurality of possible interrogation questions;

d) validating that the key is authorized to access the enclosure by comparing the enclosure identification to a list of authorized enclosure identifications stored in the key;

e) computing an interrogation response signal using a selected stored cipher variable corresponding to the interrogation question and the enclosure identification, in response to a key validation;

f) transmitting the interrogation response signal from the key to the lock controller; and

g) repeatedly transmitting power from the key to the lock controller until the key receives a signal

09392596-062701

from the lock controller indicating that sufficient power has been received by the lock controller to send an open signal to the enclosure lock.

2. The method of Claim 1, further comprising:

- a) determining a current time;
- b) determining if the key is valid at the current time; and
- c) only performing step 1(a) - 1(g) if the key is determined to be valid at the current time.

3. The method of Claim 1, further comprising:

- a) determining a current date and a current time; and
- b) transmitting the current date and the current time from the key to the electronic locking device.

4. The method of Claim 3, further comprising receiving a record of key accesses at the key from the lock controller, the record of key accesses having a list of entries for a prior time period, each entry in the list of entries having:

- a) a key identification;
- b) a time and date of attempted access for the key identification; and
- c) a status of the attempted access.

5. The method of Claim 4, further comprising a count of access attempts for a respective key identification value if a plurality of access attempts occur within a predetermined period of time.

6. The method of Claim 1, further comprising:

- a) obtaining a personal identification number for the key;
- b) validating the personal identification number for the key; and
- c) only performing 1(a) - 1(g) if the personal identification number for the key is valid.

FD-350 (Rev. 5-22-64)